Title: **System and Equipment Security Policy**

Index: 104-A

Effective Date: July 1, 2014

Revision/Date: 1/November 2017

Author: Ben Goff, Deputy Director Pima County Department of Transportation

1. **Purpose**
    a. The purpose of this document is to provide general policy guidance for PCWIN system and equipment security.

2. **Background**
    a. Because IT networks are vulnerable to attack, specific precautions must be taken to ensure that risk to the PCWIN network and equipment is mitigated to the maximum extent practical.
    b. Errors, in addition to malice, can create system failures that require prompt recovery and restoration of normal operations. A robust security environment will assure that only appropriately qualified persons, software systems and devices can access the PCWIN network.

3. **Policy Statement**
    a. Technical system information which could compromise system security is considered confidential and is not to be released to personnel who do not have a legitimate and appropriate need. Transfer of such technical information shall be accompanied by a release from the responsible owning entity and a receipt from the person to whom the technical information is provided.
    b. Network equipment is allocated to specific agencies on the system and shall not be altered by another entity without the responsible agency's knowledge and consent. Alterations require the consent of the Network Managing Member prior to implementation. Alteration includes over-the –air modifications to individual unit programming.
    c. Agencies are responsible for maintaining positive control over PCWIN equipment. Inventories of unassigned equipment shall be conducted regularly. Status of assigned equipment shall be confirmed at least annually.
    d. Additions or alterations to PCWIN software will only be allowed with the prior approval of the Network Managing Member. In general, software modifications will only be made by staff of the Network Managing Member or vendors operating under their supervision. All software documentation must be provided to the Network Managing Member in advance of software alteration or installation.
    e. The Network Managing Member is responsible for system security. A Security Protocol will be published and distributed to all PCWIN participating agencies.

f. Any facility (tower sites and facilities) will be kept secure and access will be coordinated with the Network Managing Member. All site access shall be logged with person(s), date, time and purpose.
g. Network Managing Member shall provide passwords to protect system and subsystem equipment, for the purpose of preventing unauthorized access. Specifications for required password forms and expiration intervals will be contained in the Security Protocol.
h. External devices (computers, modems, routers, external drives, iPhones, etc.) shall not be connected to the system network without the prior approval of the Network Managing Member.
i. Tower site access lists will be kept up to date, including vendor support staff. Site access lists will be honored. A person will be denied unsupervised access to a site using an access list if the person is not designated on the list for the site.
    i. Undesignated staff at equipment locations must be under the supervision of authorized staff.
        1. Agency owned sites shall control and restrict access
    ii. Notifications of urgent staff changes, such as discharged employees or cancelled vendor contracts will be immediately forwarded to the Network Managing Member. Likewise the Network Managing Member will notify clients of personnel changes that affect access to a site.
    iii. Specifics for monitoring site access alarms are at the respective site owning agency's discretion. However, at a minimum all access alarm events shall be logged.
    iv. Site access shall not be unreasonably denied to agency support staff, which is responsible for maintaining equipment located at that site.

4. Applies to

a. All users of the PCWIN digitally trunked radio system

5. Supporting Rules

a. 101-C Confidentiality Policy
b. 102-C Lost / Compromised Radio Policy
c. 202-B Lost / Compromised Radio Procedure
d. 103-B Approved Subscriber Equipment
e. 104-B Encryption Management Policy

6. Conditions for Exemption or Waiver

a. None